Strongly-Local Reductions and the Complexity/Efficient Approximability of Algebra and Optimization on Abstract Algebraic Structures(Extended Abstract)

HARRY B. HUNT III^{2,4}

Madhav V. Marathe³

RICHARD E. STEARNS²

ABSTRACT

We demonstrate how the concepts of algebraic representability and strongly-local reductions developed here and in [20] can be used to characterize the computational complexity/efficient approximability of a number of basic problems and their variants, on various abstract algebraic structures **F**. These problems include the following:

 Algebra: Determine the solvability, unique solvability, number of solutions, etc., of a system of equations on F. Determine the equivalence of two formulas or straight-line programs on F.

2. **Optimization**:Let $\epsilon > 0$.

- (a) Determine the maximum number of simultaneously satisfiable equations in a system of equations on \mathbf{F} ; or approximate this number within a multiplicative factor of \mathbf{n}^{ϵ} .
- (b) Determine the maximum value of an objective function subject to satisfiable algebraically-expressed constraints on \mathbf{F} ; or approximate this maximum value within a multiplicative factor of \mathbf{n}^{ϵ} .
- (c) Given a formula or straight-line program, find a minimum *size* equivalent formula or straight-line program; or find an equivalent formula or straight-line program of $size \leq f(minimum)$.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

ISSAC 2001, UWO, Canada

©2001 ACM 1-58113-218-2/ 00/ 0008

\$5.00

Both finite and infinite algebraic structures are considered. These finite structures include all finite non-degenerate lattices and all finite rings or semi-rings with a nonzero element idempotent under multiplication (e.g. all non-degenerate finite unitary rings or semi-rings); and these infinite structures include the natural numbers, integers, real numbers, various algebras on these structures, all ordered rings, many cancellative semi-rings, and all infinite lattices with two elements a,b such that a is covered by b.

1. INTRODUCTION AND PROBLEM STATE-MENTS

We study the complexity and approximability of a number of problems involving computations on algebraic structures, including both finite and infinite algebraic structures. Such problems arise in diverse application areas including digital circuit design, simulation, analysis, and fault-diagnosis [15] ¹, lexical analysis and code optimization of computer programs [3]², relational and logical database query processing [43]³, computational algebraic geometry and robotics [5], combinatorial and numerical optimization [21], fixed-precision numerical computation [21]⁴, model-checking and verification of finite-state processes and discrete dynamical systems [8], and the analysis of finite and discrete dynamical

¹Using our terminology, the various methods in these references for testing postulated faults in acyclic gate-level and/or transistor-level networks are equivalent to solving systems of equations on various finite lattices, where the systems of equations also result from the networks by strongly-local reductions. Our constructions actually show, that the problems of determining the testability of these various kinds of faults are strongly-local inter-reducible with the problem 3SAT, and hence, with each other.

²For example, our results on the complexity of straightline program equivalence and approximate minimization problems on the structures $\mathbf{LANG}(\{0,1\}^*)$ and $\mathbf{FIN-}$ $\mathbf{LANG}(\{0,1\}^*)$ apply directly to LEX programs.

³Our results on the complexity of formula and straightline program equivalence and approximate minimization problems on the structures **TUPLES**($\{0,1\}$) and **BIN-RELATIONS**(**U**), i.e. finite sets of k- tuples ($k \ge 1$) of 0's and 1's under the operations of \cup and cartesian product and finite binary relations on an infinite set U under the operations of \cup and composition or under the operations of \cup and join, apply directly to query processing for both relational and logic databases

⁴The proofs of our *hardness* results for solving systems of equations on various finite rings, finite semi-rings, and finite algebras also apply to solving systems of equations on the natural numbers, integers, reals, complex numbers, real and complex tensors, etc., when discretized.

¹Corresponding Author. Los Alamos National Laboratory, P. O. Box 1663, MS M997, Los Alamos NM 87545. The work is supported by the Department of Energy under Contract W-7405-ENG-36. Email: marathe@lanl.gov.

²Research supported in part by NSF Grant CCR94-06611. Department of Computer Science, University at Albany - State University of New York, Albany, NY 12222. Email: hunt,res@cs.albany.edu.

³Some of the work done while author was visiting Los Alamos National Laboratory and supported by the Department of Energy under Contract W-7405-ENG-36.

systems [38]⁵. The complexity and more recently approximability of decision and optimization of algebraic problems over various algebraic structures has been the subject of a number of recent papers. In this paper, our goals are as follows:

- 1. to demonstrate the power, wide applicability, naturalness and **simplicity** of algebraic representability and associated strongly-local reductions as developed here and in [20] in characterizing the complexities/efficient approximability of algebra and optimization over many abstract algebraic structures;
- 2. to develop techniques, concepts, and a unified methodology, for characterizing (preferably simultaneously) the complexities/efficient approximability of the problems (1)-(12) below, for many different structures, when instances are specified by standard specifications, hierarchically, periodically/dynamically, recursively, etc.;
- **3.** to develop techniques, concepts, and a *unified* methodology, for characterizing the complexity/efficient approximability of algebraic problems, that can be used to characterize complexities, ranging inclusively from **P-/ NP-**hard to *undecidable*; and
- **4.** assuming $P \neq NP$, $P \neq PSPACE$, etc., to discover how much and what kinds of *non-linearity* suffice to make solving a system of *non-linear* equations on an algebraic structure F hard.

We demonstrate simultaneously how algebraic representability and strongly-local reductions enable us to characterize in a unified way the complexity/efficient approximability, not only of the problems (1)-(12) below, but also of many of their variants obtained by varying (i) the kind of instance, e.g. formulas, straight-line programs, systems of equations, (ii) the kind of specification, e.g. hierarchical and dynamic specifications, and (iii) the class of algebraic structures on which problems are defined, or by restricting (iv) problems to bandwidth- or treewidth-bounded instances or to planar or δ -near-planar instances as defined in [4, 41, 37]. Thus for example using the concepts of algebraic representability and strongly-local reductions, we characterize simultaneously the complexity/efficient approximability of problems (1)-(12) below, for formulas, straight-line programs and acyclic networks, for systems of equations, etc., on any non-degenerate lattice with elements a,b, such that b covers a and on any ring or finite semi-ring with an element $x \neq 0$ such that $x = x \cdot x$, when specified by standard, hierarchical, or dynamic specifications. Moreover, we can characterize simultaneously both the sequential and parallel complexity of these problems. Our bounds are always tight for finite structures. Many of our bounds, for particular infinite structures, are also provably tight. Our results are summarized in Section 2 and their significance including comparison with relevant results in the literature is discussed in Section 3. Due to lack of space, additional proof sketches can be obtained from the authors.

1.1 Problems and algebraic structures considered and naming convention

Throughout this paper, **F** is an algebraic structure; and $\epsilon > 0$. We consider the following problems:

- **A. Algebra**: Let \mathcal{E} be a system of equations and F_1 , F_2 be two formulas or straight-line programs on \mathbf{F} . (1): Determine if \mathcal{E} has a solution, and if so find a solution. (2): Determine if \mathcal{E} is uniquely satisfiable. (3): Determine the number of solutions of \mathcal{E} . (4): Determine if F_1 and F_2 are equivalent, given values for f's (input) variables.
- **B. Optimization.** (5): Determine the maximum number of simultaneously satisfiable equations of a system \mathcal{E} of equations on \mathbf{F} ; and (6): approximate this maximum within multiplicative factors of ϵ or of \mathbf{n}^{ϵ} . (7): determine the maximum value of a linear objective function f on \mathbf{F} , subject to algebraically-specified constraints on \mathbf{F} ; and (8): approximate this maximum within multiplicative factors of ϵ or of \mathbf{n}^{ϵ} . (9)-(10): given a formula or straight-line program \mathcal{F} on \mathbf{F} , find a minimum size equivalent formula or straight-line program; and, (11)-(12): find an equivalent formula or straight-line program of size $\leq f(minimum)$, e.g. $(1+\epsilon)$ times minimum.

We denote the problems of determining the solvability of, unique solvability of, the maximum number of simultaneously satisfiable equations of, the maximum number of a distinguished set of variables set equal to one in a satisfying assignment of, and the cardinality of the set of solutions of a system of equations on \mathbf{F} by $SAT(\mathbf{F})$, UNIQUE-SAT(\mathbf{F}), MAX-SAT(F), MAX-DONES-SAT(F), and #-SAT(F), respectively. We denote the problems of determining the equivalence of two formulas or of two straight-line programs F_1 , F_2 on **F** by FORM-EQUIV(**F**) and SLP-EQUIV(**F**). (To simplify the statements of our results unless stated explicitly otherwise, we assume that these problems are restricted to systems of equations with no more than 1 occurrence of an operator on each side of a equation.) We denote the problems of determining the solvability of a system of linear equations on \mathbf{F} , the $\{0,1\}$ -solvability of a system of linear equations on **F**, and the feasibility of a system of linear equalities on the integers by LINEAR-SAT(F), {0, 1}-LINEAR-SAT(F), and ILP-FEASIBILITY, respectively. For these last three problems, we make no restrictions on the numbers of operators allowed on other side of equations or inequalities. We denote the problem Π , when instances are specified hierarchically as in [27, 32], etc., by H- Π . We obtain results, for both finite and infinite structures F, including: all rings or finite semi-rings with a nonzero element idempotent under , all rings without nonzero zero divisors, the natural numbers N, integers Z, real numbers R, complex numbers C, various algebras on and all bounded fixedprecision versions of the integers, reals, and complex numbers, etc., all ordered rings, many cancellative semi-rings, the sets of languages on and of finite languages on $\{0,1\}^*$ under union and concatenation, all lattices with two elements a,b such that a is covered by b, etc.

⁵ For example, we can show a direct one-to-one correspondence between paths in the *phase spaces* of finite discrete dynamical systems and satisfying assignments of dynamically-specified satisfiability problems on various finite domains. This correspondence extends directly to finite discrete dynamical systems when specified hierarchically.

2. SUMMARY OF RESULTS

We obtain both easiness results (for exact solvability and for efficient approximability) and hardness results. Examples of our results are summarized in Figure 1 and META-THEOREMS 2.1-2.2. Figure 1 summarizes the relevant complexity-theoretic properties of strongly-local reductions; and META-THEOREMS 2.1-2.2 summarize many of our results on the existence of strongly-local reductions and, consequently, the complexity/efficient approximability of the problems (1)-(12) above, for finite and for infinite algebraic structures respectively.

META THEOREM 2.1: FINITE STRUCTURES ONLY.

- I. General Efficient Approximations for Finite Structures: Let F be any finite algebraic structure.
- 1. There exists $\epsilon > 0$ such that the problems of approximating the maximum numbers of simultaneously satisfiable equations in a system of equations, in a system of hierarchically-specified equations, or in a system of dynamically-specified equations on \mathbf{F} , with ϵ times optimum are solvable in polynomial time.
- **2.** For all $\delta > 0$, there exists a **PTAS**, for approximating the problem MAX- SAT(**F**), when this problem is restricted to δ -near-planar instances.
- **3.** For all finite (not necessary total) algebraic structures \mathbf{F} , there exists an integer $k \geq 1$ such that the problem SAT(\mathbf{F}) is (k-strongly-local+parsimonious+L)- reducible to the problem 3SAT. ⁸
- II. General Hardness Results for Finite Structures: Let \mathbf{F} be any finite non-degenerate lattice or any finite ring or semi-ring for which $\exists x \in \mathbf{F}$ such that $\forall n \geq 1$, $x^n \neq 0$. Then, the problem 3SAT is (2- or 1-stronglylocal+parsimonious+L)-reducible to the problem SAT(\mathbf{F}).

⁶Since the maximization versions of many of these optimization problems, when instances are specified hierarchically or by various kinds of dynamic specifications are **PSPACE**, **DEXPTIME**, **NDEXPTIME**, **EXSPACE**-hard, or even undecidable [31], we see that our concepts and techniques can also be used to develop efficient approximation algorithms, for natural algebraic optimization problems ranging in complexity from **NP**-hard to undecidable. Previous to our work, no such general general easiness results were known, for natural provably hard problems, much less for

⁷By **PTAS** we mean a polynomial time approximation scheme as defined in [14]. All of these schemes are actually **NC** approximation schemes. Recalling the previous footnote, this result yields a natural infinite collection of provably hard optimization problems with **NC** approximation schemes. Previously, no such general infinite class of natural provably hard, as opposed to likely hard(e.g. **NP**-hard), but arbitrarily efficiently approximable problems was

such large classes of natural provably hard problems.

⁸We say that problem Π_1 is " $(\alpha+\beta+\gamma)$ -reducible" to problem Π_2 if and only if Π_1 is reducible to Π_2 by a single reduction, that is *simultaneously* an α , a β , and a γ reduction.

Consequently, the following hold:

- 4. The problem SAT(F) is both NQL- and $\leq_{\log n}^{\mathbf{bw}}$ -complete for NP; the problem #-SAT(F) is #P-complete; and the problems MAX-SAT(F) and MAX-DONES-SAT(F) are MAX-SNP- and MAX- Π_1 -complete, and thus, have NP-hard ϵ and \mathbf{n}^{ϵ}) approximation problems [6, 35].
- 5. The problem H-3SAT is (2- or 1-strongly-local+parsimonious+L)-reducible to the problem H-SAT(F). Consequently, the problems H-SAT(F) and H-#-SAT(F) are PSPACE- and #PSPACE-complete, Also there exist $\epsilon > 0$ such that approximating the problems H-MAX-SAT(F) and H-MAX-DONES-SAT(F) within ϵ times maximum and within \mathbf{n}^{ϵ} times maximum, respectively, are PSPACE-complete. ¹⁰

META THEOREM 2.2: INFINITE STRUCTURES

Let $\epsilon > 0$. Let **F** be an algebraic structure.

- 1. There exists $\epsilon > 0$ such that the problem SAT(F) is 1-strongly-local reducible to the problem of approximating the maximum number of simultaneously satisfiable equations of a system of equations on F within n^{ϵ} times maximum. (Here, we place no restrictions on he numbers of operators appearing on the sides of the equation.)
- 2. Suppose $0 \in \mathbf{F}$. Let Π be the problem of determining if a formula on \mathbf{F} denotes the constant function 0. For all functions $f: \mathbf{N} \{0\} \to \mathbf{N} \{0\}$, the problem Π is 1-strongly-local reducible to the problem of finding an equivalent formula of size $\leq f(min)$, where min is the size of an equivalent formula of minimum size.
- **3.** The problems FORM-EQUIV(FIN-LANG($\{0,1\}^*$)) and SLP-EQUIV(FIN-LANG($\{0,1\}^*$)) are **coNP** and **coNDEXPTIME**-complete, respectively. 11
- 4. [Complexity of ILP Feasibility and Real-Closed Fields, Restricted to Bandwidth- or Treewidth-Bounded Instances:] There exists a fixed integer $k \geq 1$ such that the problems ILP-FEASIBILITY and SAT($\mathbf{R}_{\mathcal{A}}$) are weakly-NP-complete, when restricted to systems of linear constraints and algebraic equations with integer coefficients on $\mathbf{R}_{\mathcal{A}}$ with bandwidth and/or treewidth $\leq k$. Unless

¹⁰The counting complexity class **#-PSPACE** defined by [26] is the analogue for **PSPACE** of the counting complexity class **#P** for **NP**.

¹¹Thus there is a *provable* exponential gap between the complexities of the formula- and of the straight-line-program-equivalence problems, for these structures. By direct expansion, there is at most a singly exponential gap between the complexities of these two problems, for any abstract algebraic structure **F**.

⁹The concepts of **NQL**- and $\leq_{\log n}^{\mathbf{bw}}$ -completeness are stronger than the concept of **NP**-completeness and are defined in [40, 41], respectively. The concepts of #P-, **MAX**-**SNP**-, and **MAX**-Π₁-completeness are defined in [44, 36, 35], respectively.

P=NP, these problems are not strongly-NP-complete. ¹²

5. [Results for Ordered Rings or Cancellative Semi-Rings]: Let **F** be any ordered unitary ring or cancellative semi-ring, that is the non-negative part of an ordered unitary ring. Then the problem SAT(**F**) is 1-strongly-enforcer or 1-strongly-local bounded tt-reducible¹³ to each of the following problems:

i. UNIQUE-SAT(F); ii. for all k > 1 determine if a system of equations on **F** has exactly k or has $\geq k$ distinct solutions; iii. determine if a system of equations on F has an infinite number of solutions; iv. determine the maximum number of simultaneously satisfiable equations in a system of equations on **F**; **v**.there exists $\epsilon > 0$ approximating the maximum number of simultaneously satisfiable equations of a system of equations on \mathbf{F} within \mathbf{n}^{ϵ} times maximum; vi.determine the maximum value (MAX) taken on by a linear objective function subject to satisfiable equational constraints on F; and vii. there exists $\epsilon > 0$ such that approximating the maximum taken on by a linear objective function subject to satisfiable equational constraints on \mathbf{F} within \mathbf{n}^{ϵ} times maximum. Moreover for any ordered ring F, viii.the problem $SAT(\mathbf{F})$ is (1-strongly-local+ parsimoniously)-reducible to the problem of determining if a 4th degree multiple-variable polynomial on F has roots in F. Finally letting F equal N or **Z**, there are no algorithms, for any of the problems **i-viii**. (These last undecidability results follow immediately from the results for the problems of i-viii and the well-known undecidability of Hilbert's 10th problem [33, 12]. Among other things, these undecidability results generalizes Jeroslow's result [23], that there is no algorithm, for integer programming subject to quadratic constraints, by showing that there are also no algorithms for approximating integer programming subject to quadratic constraints.)

All of the strongly-local reductions and consequent hardness results of items 4 and 5 of META-THEOREM 2.1, for the problems SAT(F) and MAX-SAT(F), also hold for any ring or finite semi-ring with a non-zero element xsuch that $x^2 = x$. In addition all of the strongly-local reductions and consequent hardness results of items 4 and 5 of META-THEOREM 2.1, for the problems SAT(F), #-SAT(F), and MAX-SAT(F), also hold, for the following: (a) any infinite lattice with elements a,b where a is covered by b, (b)any infinite ring with no non-zero zero divisors, and (c)the problems LINEAR-SAT(N), {0,1}-LINEAR-SAT(N), and ILP-FEASIBILITY. Moreover, there exists an $\epsilon > 0$ such that approximating the maximum value of a linear objective function on Z subject to linear constraints and to hierarchically-specified linear inequality constraints on **Z** within n^{ϵ} times maximum are **NP**-hard and PSPACE-hard, respectively.

7. The problem 3SATWP is 1-strongly-local and A-reducible 14 to the problem LPFEASIBILITY. Consequently since the problem H-3SATWP is **PSPACE**-hard and there exists $\epsilon > 0$ such that approximating the problem H-MAX-DONES-3SATWP within a multiplicative factor of n^{ϵ} times maximum is also **PSPACE**-hard, so are the the problems of approximating the maximum value of a linear objective function on **Q** subject to satisfiable hierarchically-specified linear inequality constraints on **Q**.

3. SIGNIFICANCE

The following additional properties of results/constructions/techniques are also of interest.

- 1. Usually the formulas, straight-line programs, systems of equations, recursive function specifications, etc. , occuring in our proofs contain *only* a bounded number of distinct constants. Moreover, usually the only properties of these constants used are properties that hold, for each algebraic structure of the same kind, e.g. the properties of the additive and multiplicative identities common to all *unitary* rings or semi-rings. This enables us to obtain complexity results, for a structure that are *independent* both of the structure's presentation and its cardinality.
- 2. By restricting ourselves to strongly-local reductions, we know a priori, that all properties of Meta-Result 1 hold for them. Thus for example, we know that our reductions relate simultaneously both the sequential and parallel complexities of problems, when instances are specified straight-line programs, acyclic computational networks, systems of equations, hierarchically- and recursively-specified functions and systems of equations, periodically-specified formulas and systems of equations, etc. One immediate implication is that all of the hardness results in [31], for the problems 3SAT and 3SATWP, when instances are specified by various kinds of dynamic/periodic specifications, also hold, for the problems SAT(F), #-SAT(F), MAX-SAT(F), UNIQUE-SAT(F), etc. and for the algebraic structures in items 4 of Meta-Theorem 2.1 and 4, 5, 6, and 7 of Meta-Theorem 2.2, when instances are specified by the corresponding kinds of dynamic/periodic specifications.
- 3. Often our proofs, for rings and semi-rings, do not require that the binary operations + and \cdot actually be total, associative, or commutative. One direct implication of this is that—
 - Our hardness results, for finite rings and semi-rings, also hold, for discretized bounded-precision versions of the natural numbers, integers, rationals, reals, Gaussian integers, complex numbers, tensors on these structures, etc. Due to under-flow and over-flow, these discretized bounded-precision versions are actually neither rings nor semi-rings.
- 4. [Some General Complexity Theoretic Implications:] The variant problems, for several basic algebraic structures **F**, provide natural yardsticks, for measuring complexity and/or

¹²Let $k \ge 1$ be a fixed integer. Assuming $\mathbf{P} \ne \mathbf{NP}$, this results shows, that the known polynomial time algorithms for ILP and for solving a system of equations on $\mathbf{R}_{\mathcal{A}}$, for instances with $\le k$ variables [5, 28], cannot be extended (while remaining polynomial time bounded) to apply to instances of bandwidth or of treewidth $\le k$.

¹³Here, tt stands for truth-table. These more general variants of strongly- local reductions have essentially the same complexity-theoretic properties as pure strongly-local reductions.

 $[\]overline{^{14}\text{The concept}}$ of A-reducibility defined in [35] is stronger than the concept of L-reducibility

efficient approximability. They play roles in characterizing the complexities of algebraic and numerical optimization strongly analogous to the roles played by the problems 3SAT, MAX-3SAT, MAX-DONES-3SAT, #-3SAT, in characterizing the complexity or efficient approximability of combinatorial problems (e.g. in [14, 36, 35]). By using infinite structures **F**, we can obtain results for higher levels of complexity including undecidability. Thus recalling items 1,2,5, and 7 of META-THEOREM 2.2, our results are a significant step towards finding general techniques that can be used to simultaneously prove lower bounds from **NP** to **NDEXPTIME** and even to **Undecidability**.

- 5. [Progress on open questions in the literature:] Our results significantly extend earlier results and are a strong step towards answering open questions in the literature. Specific questions related to our work include: (i) Ladner [26] to identify new natural #PSPACE-hard and -complete counting problems;
- (ii) Condon et al. [9, 10] to identify natural classes of **PSPACE**-hard optimization problems with provably **PSPACE**-hard ϵ -approximation problems, and the results of [25, 11] providing dichotomy results for the problems MAX SAT(**S**).
 - Our general techniques simultaneously imply the MAX-SNP-hardness and MAX-Π₁-hardness of the problems MAX-SAT(F) and MAX-DONES-SAT(F) and the PSPACE-hardness of approximating the problems H-MAX-SAT(F) and H-MAX-DONES-SAT(F), for suitable large ε < 1 and for all ε > 0 respectively, over infinitely many non-isomorphic algebraic structures including all those of items 4 and 6 of META-THEOREMS 2.1 & 2.2, respectively. No analogous such general results were known previously.
- (iii) Zuckerman [45] on **NP**-hardness of constrained problems to **PSPACE**-hardness of approximating succinctly specified constrained optimization problems; and
 - Our results show that most of Zuckerman's hardness results, for approximation problems, are actually implied by strongly-local reductions of the problem UNIQUE-3SAT. Consequently among other things, we get analogous hardness results, for these approximation problems when restricted to planar or UD instances and when instances are specified hierarchically, dynamically/periodically, etc.
- (iv) the results of Khanna and Motwani [24], our results [17] and those of Trevisan [42] on (NC)-PTAS for MAX SAT(S) restricted to planar and near-planar instances.
 - We show that PTASs exist, for the problem MAX-SAT(F) restricted to near-planar instances, for all finite algebraic structures; and that this is an immediate implication of our earlier PTAS for the problem PL-MAX-3SAT in [17].

- (v) Our strongly-local L- and strongly-local A-reductions of the problems MAX-3SAT and MAX-DONES-3SAT to the problems MAX-SAT(\mathbf{F}) and MAX-DONES-SAT(\mathbf{F}), respectively, for all structures \mathbf{F} satisfying items 4 and 8 of META-THEOREMS 2.1 & 2.2, respectively, significantly extend the collection of natural problems known to be hard to approximate (assuming $\mathbf{P} \neq \mathbf{NP}$).
- 6. Direct analogues of our hardness results, for approximating minimum equivalent formulas, also hold for other classes of algebraic, logical, or linguistic descriptors including 3CNF formulas, Boolean formulas and acyclic Boolean networks, quantified Boolean formulas, regular expressions, nondeterministic FSA, nondeterministic PDA, CFGs, etc. Thus for example, all f(min)-bounded approximations for minimum equivalent 3CNF formulas, Boolean formulas and acyclic Boolean networks, quantified Boolean formulas are expressions, nondeterministic FSA, nondeterministic PDA, and CFGs are intuitively as hard as the corresponding satisfiability or "= $\{0,1\}$ *" problems. Thus all approximations for these problems are coNP-, coNP-, PSPACE-, PSPACE-hard, have no algorithms, respectively.
- 7. Our strongly-local reductions for ordered rings and semirings in item 6 of Meta-Theorem 2.2 problem instances with $m \leq 1$ variables into problem instances with O(m), and in some cases, with m+O(1) variables. In which case, these reductions also preserve upper bounds of the form –Problem II is solvable deterministically in polynomial time, for problem instances with a fixed number of variables, where the degree of the polynomial upper bounds grows polynomially, linearly, quadratically, etc., in the number of variables occurring in the instance. (Recall that such upper bounds are known for solving systems of polynomial equations on $\mathbf{R}_{\mathcal{A}}$.)
- 8. Assuming $\mathbf{P} \neq \mathbf{NP}$, we can show that the conditions of items 4 and 8 of Meta-Theorems 2.1 and 2.2 are not necessary for the hardness of the problem SAT(\mathbf{F}). In fact, we can show the \mathbf{NP} -hardness of the problem SAT(\mathbf{F}), for finite structures \mathbf{F} such that both $\forall x \in \mathbf{F}$, $x^2 = 0$ and $\forall x, y, z \in \mathbf{F}$, $x \cdot y \cdot z = 0$. These additional hard rings include rings of differential forms on vector spaces over finite fields; and thus, they may be of independent interest. Additionally for all ordered rings \mathbf{F} ,we can show that the the problem 3SAT is (1-strongly-local+parsimonious+L)-reducible to the problem of determining if a system of peice-wise linear equations on \mathbf{F} has a solution. These two results show how little non-linearity is required, for the problem of determining if a system of non-linear equations on \mathbf{F} to be hard.

4. OVERVIEW OF TECHNOIUES

The concepts and methodology used here are based upon the concepts of algebraic representability (a modification for algebraic structures of the concept of relational representability as defined in [39, 20]) and strongly-local replacements/reductions defined in [20] as extended here to apply to the problems SAT(\mathbf{F}), #-SAT(\mathbf{F}), MAX-SAT(\mathbf{F}), etc., for various abstract algebraic structures \mathbf{F} . Recall that unless stated explicitly otherwise, we restrict our attention to systems of equations with ≤ 1 occurrence of an operator on each side of an equation. We note that—

• For all fixed integers $k \geq 1$, exactly analoguous results hold, when we restrict our attention to systems of equations with $\leq k$ occurrences of operators on each side of an equation or comparison operator.

For each algebraic structure **F** considered, there exist distinct constants a_1, \ldots, a_k $(k \ge 0)$ such that, the only constants appearing in the formulas, straight-line programs, systems of equations, etc., on **F** occurring in our proofs are the a_i $(1 \le i \le k)$. Usually $k \le 2$.

- 1. Algebraic/Relational Representability: Let \mathbf{F}_1 and \mathbf{F}_2 be algebraic structures with domains D_1 and D_2 , finite sets of finite- arity operators $\{o_{1,1},\ldots,o_{1,r^1}\}$ and $\{o_{2,1},\ldots,o_{2,s^1}\}$, and finite sets of allowed constants $\{a_{1,1},\ldots,a_{1,r^2}\}$ and $\{a_{2,1},\ldots,a_{2,s^2}\}$, respectively. For simplicity here, we assume that all of these operators are binary. We define the sets $\mathbf{S}_{\mathbf{F}_1}$ and $\mathbf{S}_{\mathbf{F}_2}$ of relations (on D_1 and D_2) defined by \mathbf{F}_1 and \mathbf{F}_2 , respectively, as follows:
 - 1. $\mathbf{S_{F_1}}$ consists of the following set of relations on D_1 : $\mathbf{R}_{1,0} = \{(x,y) \mid x,y \in D_1 \text{ and } x = y\}$, for all constants $\mathbf{a}_{1,l}$ in D_1 , $\mathbf{R}_{a_{1,l}} = \{a_{1,l}\}$, and for all operators $\mathbf{o}_{1,j}$, $\mathbf{R}_{o_{1,j}} = \{(x,y,z) \mid x,y,z \in D_1 \text{ and } z = o_{1,j}(x,y)\}$.
 - 2. $\mathbf{S}_{\mathbf{F}_{2}}$ consists of the following set of relations on D_{2} : $\mathbf{R}_{2,0} = \{(a,b) \mid a,b \in D_{2} \text{ and } a = b\}$, for all constants $\mathbf{a}_{2,l'}$ in D_{2} , $\mathbf{R}_{a_{2,l'}} = \{a_{2,l'}\}$, and for all operators $\mathbf{o}_{2,j'}$, $\mathbf{R}_{c_{2,j'}} = \{(a,b,c) \mid a,b,c \in D_{2} \text{ and } c = c_{2,j'}(a,b)\}$.

Algebraic/relational representability formalizes the intuitive concept that the relations in $\mathbf{S}_{\mathbf{F}_1}$ are *expressible* (or extending the terminology from [39] are *representable*) by finite conjunctions of the relations in $\mathbf{S}_{\mathbf{F}_2}$.

Definition 4.1. We say that \mathbf{F}_1 is algebraically-representable by \mathbf{F}_2 if and only if, there exists a 1-1 function $\Phi: D_1 \to D_2$ such that, for all relations R(x), R(x,y), or $R(x,y,z) \in \mathbf{S}_{\mathbf{F}_1}$, there exists a finite conjunction $\mathbf{C}_{R(x)}$, $\mathbf{C}_{R(x,y)}$, or $\mathbf{C}_{R(x,y,z)}$, of relations in $\mathbf{S}_{\mathbf{F}_2}$ applied to the variable(s) x, or x,y, or x,y,z, respectively, additional existentially-quantified variables, and constants of \mathbf{F}_2 such that,

- letting \mathbf{X}_R be the set of tuples of elements of D_1 that satisfy relation R and letting \mathbf{Y}_R be the projection of the set of tuples of elements of D_2 that satisfy conjunction $\mathbf{C}_{\mathbf{R}}$ on their first, first and second, or first, second, and third components, $\mathbf{X}_{\mathbf{R}} = \Phi^{-1}(\mathbf{Y}_{\mathbf{R}})$.
- 2. Local Replacements: Let $k \geq 1$. The second basic component of our methodology consists of the formalization and systematic investigation of the properties of the classes of k-strongly-local and k-strongly-local-enforcer replacements and reductions, to the problems $SAT(\mathbf{F})$, #- $SAT(\mathbf{F})$, MAX- $SAT(\mathbf{F})$, etc. Meta-Result 1 in Figure 1

$$\begin{array}{lll} \overline{^{15}\mathrm{Here}, & \Phi^{-1}((a)) & := & (\Phi^{-1}(a)), & \Phi^{-1}((a,b)) & := \\ (\Phi^{-1}(a), \Phi^{-1}(b)), & \mathrm{and} & \Phi^{-1}((a,b,c)) & := \\ (\Phi^{-1}(a), \Phi^{-1}(b), \Phi^{-1}(c)). & & & \end{array}$$

summarizes the complexity-theoretic properties of these reductions. ¹⁶ Here, we only describe 1-strongly-local and 1-strongly-local enforcer reductions intuitively.

Let $\mathcal{E} = (eq_1, \dots, eq_m)$ with $m \geq 1$ be a finite sequence of equations $\langle lhs \rangle = \langle rhs \rangle$ on F, where no more than one operator of **F** occurs in $\langle lhs \rangle$ and no more than one operator of F occurs in $\langle rhs \rangle$. Using distinct new temporary variables, we can replace each such equation by a fixed size conjunction of relations in the set $S_{\mathbf{F}}$, i.e. the relations defined by \mathbf{F} . Let \mathbf{F} and \mathbf{F}' be distinct algebraic structures. We define k-strongly-local and k-strongly-local-enforcer reductions of the problem $SAT(\mathbf{F})$ to the problem $SAT(\mathbf{F}')$ to be k-strongly-local and k-strongly-local-enforcer replacements from the set of all finite sequences of relations in S_F to the set of all finite sequences of relations in $S_{\mathbf{F}'}$, that are also reductions. Intuitively, $\forall k$, in k-strongly-local replacements we have templates, to be treated as macros, with the same template for each variable and distinct templates for each relation in $S_{\mathbf{F}}$. Details about macro expansions and the the way the variables are replaced depend very simply on the value of k.

Specifically, this reduction is specified by t templates $Temp_1, \dots Temp_t$, one for each of the relations T_1, \dots, T_t in the set $S_{\mathbf{F}}$, plus (optionally) one template $Temp_v$ (the variable template) corresponding to the variables as follows: Let $f = T_{i_1} \wedge \ldots \wedge T_{i_m}$ $(m \geq 1)$ be a conjunction of the relations in S_T applied to the variables x_1, \ldots, x_n $(n \geq 1)$. The formula g = R(f) is the conjunction of the $Temp(T_{i_j})$ for $1 \leq j \leq m$ optionally anded with one occurrence of $Temp_v$ for each variable x_i $(1 \le i \le n)$ of f. Here, $Temp(T_{i_j})$ is specified as follows: Let T_{i_j} be the relation T_{ℓ} (1 $\leq \ell \leq t$). Let the variables occurring in T_{i_i} in order be x_{j_1}, \ldots, x_{j_m} . Then the (dummy) variables of $Temp_{\ell}$ are in order $z_{j_1}, \ldots, z_{j_m}, v_{1, \ldots}, v_{m_{\ell}}$ and $Temp(T_{i_j})$ results from $Temp_{\ell}$ by replacing all occurrences of the variables z_{j_1}, \ldots, z_{j_m} by occurrences of the of the variables x_{j_1}, \ldots, x_{j_m} , respectively, and by replacing all occurrences of the variables v_1, \ldots, v_{m_ℓ} by new variables w_1, \ldots, w_{m_ℓ} respectively, local to the conjunction $Temp(T_{ij})$. We call such an "intuitively" local reduction a 1-strongly local reduction. More generally ,a $k \geq 2$ -strongly local reduction is specified analogously except that each of the variables v_i is replaced by k new variables z_j^1, \ldots, z_j^k and each of the variables x_j in $Temp(T_{i_j})$ is replaced by k new variables x_j^1,\ldots,x_j^k . Formal definitions of these concepts can be found in [20].

The concepts of algebraic representability and strongly-local reductions combine together naturally as illustrated by the following theorem:

THEOREM 4.2. Let \mathbf{F}_1 and \mathbf{F}_2 be algebraic structures such that \mathbf{F}_1 is algebraically representable by \mathbf{F}_2 . Then, the problem $SAT(\mathbf{F}_1)$ is 1-strongly-local reducible to $SAT(\mathbf{F}_2)$. ¹⁷.

¹⁶In contrast, previous researchers, e.g. [14], have discussed the intuitive concept of reductions by *local replacement*; but they have *not* gone far in formalizing, or in characterizing the complexity-theoretic properties of, their concepts.

¹⁷In [20], we present a similar theorem relating the concepts of relational representability and 1-strongly-local reductions

- 1. They are simultaneously $O(n \cdot logn)$ time, linear size-, and O(logn) space-bounded on deterministic multiple-tape Turing machines; and they are NC(1) using only O(n) processors.
- 2. They preserve treewidth- and (often) bandwidthbounds. They can also be modified easily to preserve near-planarity.
- 3. They extend directly to efficient reductions, when instances are specified by straight-line programs, hierarchically, recursively, or dynamically, as defined in [27, 32, 34].

Figure 1: Meta-Result 1. Some Basic Properties of Strongly-Local Reductions.

5. TERMINOLOGY AND SELECTED DEF-INITIONS

Generally, we consider homogeneous total algebraic structures S = (S, +,) with two binary operations + and +called addition and multiplication, respectively. We assume that structures are non-degenerate, i.e. have at least two elements. We restrict our attention to such algebraic structures having only a finite set of operators, each operator of which is itself of finite-arity. The additive (multiplicative) identity of S, when it exists, is usually denoted by 0 (by 1). We define ring as in [30], except that we do not require rings to have multiplicative identities. We define $semi-ring \mathbf{F}$ by $\mathbf{F} = (S, +, \cdot, 0)$, where + is an associative and commutative binary operation on S and is an associative binary operation on S that distributes over + on both the left and the right. We say that a ring or semi-ring is unitary iff it has a 1. [NOTE: Thus unlike [30, 13], we do not assume that all rings or all semi-rings have a 1.] A ring or semi-ring ${\bf R}$ is said to cancellative iff, for all $x,y,z \in \mathbf{R}$, $x \cdot y = x \cdot z$ implies x = 0 or y = z.

We denote the problem of determining if a 3CNF formula with exactly 3 non-negated literals/clause, has a satisfying assignment satisfying exactly 1 literal per clause by Exactly1-ex3MONOTONESAT. **NOTE:** The problems 3SAT and Exactly1-ex3MONOTONESAT are known to be 1-strongly-local inter-reducible by reductions that are also parsimonious and L [20]. Finally, see [36, 35, 16] for the definitions of L- and A-reductions and the respective complexity classes **MAX-SNP-** and **MAX-** Π_1 .

6. SELECTED PROOF SKETCHES

We present several general theorems on the complexities of determining the solvability of systems of equations over various finite lattices, rings, and semi-rings. When we restrict our attention to finite structures, we assume that in each case we have a set of constant symbols, denoting in a one-to-one fashion, the elements of the structure. Recall that a lattice $\mathbf{L} = (\mathbf{S}, \wedge, \vee)$ is an algebraic structure where the operations \vee and \wedge are binary operations on \mathbf{S} that are commutative, associative, and idempotent, such that for all $x, y \in \mathbf{S}$,

$$x \lor (x \land y) = x \land (x \lor y) = x.$$

Finally, recall that an element a of a lattice **L** "is covered by" an element b of **L** if a < b in the partial order defined by the operations of **L**; and there is no element c of **L** such that a < c < b [7, 30].

Theorem 6.1. For all lattices **L** with elements a and b and constant symbols A and B denoting a and b, respectively, such that a "is covered by" b, the problem Exactly1-3MONOTONESAT is (2-strongly local+parsimonious+planarity-preserving)-reducible to the problem SAT(**L**).

Proof sketch: Let $n, m \geq 1$ be integers. Let $f = c_1 \wedge \ldots, c_m$ be a monotone 3CNF Boolean formula with exactly 3 literals per clause with distinct variables x_i $(1 \leq i \leq n)$. Let y_i $(1 \leq i \leq n)$ be n distinct new variables. The resulting system of equations EQ(f) on \mathbf{L} is given by –

- 1. $\forall i, 1 \leq i \leq n, A \leq x_i, y_i \leq B$ (i.e. $x_i \land A = A, x_i \lor B = B,$ etc.)
- 2. $\forall i, 1 \leq i \leq n, x_i \wedge y_i = A \text{ and } x_i \vee y_i = B.$
- 3. $\forall j, 1 \leq j \leq m$, let $c_j = x_{j_1} \vee x_{j_2} \vee x_{j_3}$, then EQ(f) also includes the equations— $(x_{j_1} \vee x_{j_2} \vee x_{j_3}) = B$, $(x_{j_1} \wedge x_{j_2}) = A$, $(x_{j_1} \wedge x_{j_2}) = A$, and $(x_{j_2} \wedge x_{j_3}) = A$.

We claim that "there is an assignment of truth-values to the variables of f such that exactly 1 literal in each clause is satisfiable" iff "EQ(f) is satisfiable." This is implied by noting the following:

- 1. By assumption, B covers A, thus $A \leq C \leq B$ implies C = A or C = B.
- 2. Given this, for all assignments of values from L to the variables x_i , y_i satisfying the equations of items 1 and 2 and for each i with $1 \le i \le n$, one of x_i and y_i takes on the value A and the other takes on the value B.
- 3. Given the above, any assignment of values from L to the variables x_i , y_i causes exactly one of the (nonnegated) literals in each of the clauses of EQ(F) to equal B and the other two (non-negated) literals to equal A.

Finally, it's *not* hard to see that this reduction is (2-strongly-local+parsimonious). to see why it is also preserves planarity of instances.

7. REFERENCES

- S. Arora, L. Babai, J. Stern and Z. Sweedyk. The hardness of approximate optima in lattices, codes and systems of linear equations. *Journal of Computer and System* Sciences (JCSS), 54(2), pp. 317-331, 1997.
- [2] E. Amaldi and V. Kann. The complexity and approximability of finding maximum feasible subsystems of linear relations. *Theoretical Computer Science (TCS)* 147(1&2), pp. 181-210, 1995.
- [3] A.V.Aho, R.Sethi, and J.D.Ullman. Compilers principles, techniques, and tools, Addison Wesley, Reading, MA, 1986.
- [4] S. Arnborg, J. Lagergren, and D. Seese. Which problems are easy for tree-decomposable graphs? J. Algorithms, 12, 1991, pp. 308-340.

- [5] D. Arnon and B. Buchberger (Editors), Algorithms in Real Algebraic Geometry, Academic Press, London, 1988.
- [6] S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy. Proof verification and hardness of approximation problems. J. of the ACM (JACM), 45, 1998, pp. 501-555.
- [7] G.Birkhoff, Lattice theory, (3rd ed.), American Mathematics Society, Providence, RI, 1966.
- [8] E. Clarke, O. Grumberg, and D. Peled. Model checking. Preliminary unpublished version, 1998.
- [9] A. Condon, J. Feigenbaum, C. Lund and P. Shor. Probabilistically checkable debate systems and approximation algorithms for PSPACE-hard functions. Chicago Journal of Theoretical Computer Science, Vol. 1995. No. 4.
- [10] A. Condon, J. Feigenbaum, C. Lund and P. Shor. Random debaters and the hardness of approximating stochastic functions. SIAM J. Computing (SICOMP), 26, 1997, pp. 369-400.
- [11] N. Creignou. A dichotomy theorem for maximum generalized satisfiability problems. J. of Computer and System Sciences (JCSS), 51, 1995, pp. 511-522.
- [12] M. Davis. Hilbert's tenth problem is undecidable. American Mathematical Monthly (AMM), 1973.
- [13] S. Eilenberg, Automata, languages, and machines, vol. A, Academic Press, NY, 1974.
- [14] M. Garey and D. Johnson. Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman, San Francisco, 1979.
- [15] J.P. Hayes. Digital simulation with multiple logic values. IEEE Trans. Computer-Aided Design, 1986, pp. 274-283.
- [16] D. Hochbaum(Ed.). Approximation algorithms for NP-hard problems, PWS Publishing Company, Boston, MA, 1997.
- [17] H. Hunt III, M. Marathe, V. Radhakrishnan, S. Ravi, D. Rosenkrantz and R. Stearns, Parallel Approximation Schemes for a Class of Planar and Near Planar Combinatorial Optimization Problems, to appear in Information and Computation, 2001.
- [18] H.B. Hunt III, M.V. Marathe, V. Radhakrishnan, and R.E. Stearns. The complexity of planar counting problems. SIAM J. Computing (SICOMP) Vol. 27, 1998, pp. 1142-1167.
- [19] H.B. Hunt III and R.E. Stearns. Nonlinear algebra and minimization on rings are "hard". SIAM J. on Computing (SICOMP) Vol. 16, 1987, pp. 910-929.
- [20] H.B. Hunt III, R.E. Stearns, and M.V. Marathe. Relational representability, local reductions, and the complexity of generalized satisfiability problems. Submitted for publication, 2000.
- [21] E. Isaacson and H. Keller. Analysis of Numerical Methods. Dover Publishing, NY, 1994. This is a corrected unabridged republication of the work under the same title by John Wiley & Sons, NY, 1966.
- [22] P. Jeavons, D. Cohen and M. Gyssens. Closure properties of constraints. J. of the ACM, (JACM) 44(4):527-548, July 1997.
- [23] R. Jeroslow. There cannot be any algorithm for integer programming with quadratic constraints. *Operations Research (OR)*, 21, pp. 221-224.
- [24] S. Khanna, and R. Motwani, "Towards a syntactic characterization of PTAS," Proceedings, 28th Annual ACM Symposium on Theory of Computing (STOC), pp. 329-337, 1996.
- [25] S. Khanna, M. Sudan and D. Williamson. A complete classification of the approximability of maximization problems derived from Boolean constraint satisfaction. *Proc. 29th Annual ACM Symposium on Theory of Computing (STOC)*, El Paso, TX, May 1997, pp. 329-337.
- [26] R. Ladner. Polynomial space counting problems. SIAM J. Computing (SICOMP), 18(6):1087-1097, December 1989.

- [27] T. Lengauer and K. Wagner. The correlation between the complexities of non-hierarchical and hierarchical versions of graph problems. J. Computer and System Sciences (JCSS), Vol. 44, 1992, pp. 63-93.
- [28] H.W. Lenstra, Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8, 1983, pp. 538-548.
- [29] D. Lichtenstein. Planar formulae and their uses. SIAM J. Computing (SICOMP), Vol 11, No. 2, May 1982, pp. 329-343.
- [30] S. MacLane and G. Birkhoff, *Algebra*, Macmillan, NY 1967.
- [31] M. Marathe, H. Hunt III, D. Rosenkrantz and R. Stearns. Theory of periodically specified problems:complexity and approximability. *Proc. 13th IEEE Conf. on Computational Complexity.* 1998.
- [32] M. Marathe, H. Hunt III, R. Stearns and V. Radhakrishnan. Approximation Algorithms for PSPACE-Hard Hierarchically and Periodically Specified Problems. SIAM J. Computing (SICOMP), 27(5), pp. 1237-1261, Oct. 1998.
- [33] Y. Matiyasevic, Enumerable sets are Diophantine(Russian). Dokl. Akad. Nauk SSSR, 191, 1970, pp.279-282. Improved English translation:Soviet Math. Doklady, 11, 1970, pp. 354-357.
- [34] J. Orlin. The Complexity of dynamic/periodic languages and optimization Problems. Sloan W.P. No. 1679-86 July 1985, Working paper, Alfred P. Sloan School of Management, MIT, Cambridge, MA 02139. A Preliminary version of the paper appears in Proc. 13th ACM Annual Symposium on Theory of Computing (STOC), 1978, pp. 218-227.
- [35] A. Panconesi and D. Ranjan. Quantifiers and approximations. Theoretical Computer Science (TCS), 107, 1993, pp. 145-163.
- [36] C. Papadimitriou and M. Yannakakis. Optimization, approximation, and complexity classes. J. Computer and System Sciences (JCSS), 43, 1991, pp. 425-440.
- [37] V. Radhakrishnan, H.B. Hunt III, and R.E. Stearns. Efficient algorithms for δ -near-planar graph and algebraic problems. *Complexity in Numerical Optimization*, (Edited by P.M. Pardalos), World Scientific Publishing Co., 1993, pp. 323-350.
- [38] C. Robinson. Dynamical Systems Stability, Symbolic Dynamics, and Chaos Second Edition. CRC Press, Boca Raton, Florida, 1999.
- [39] T. Schaefer. The complexity of satisfiability problems. Proc. 10th Annual ACM Symposium on Theory of Computing (STOC), 1978, pp. 216-226.
- [40] C. Schnorr. Satisfiability is quasilinear complete in NQL. J. of the ACM (JACM), 25(1):136-145, January 1978.
- [41] R. Stearns and H. Hunt III. An algebraic model for combinatorial problems. SIAM J. Computing (SICOMP), Vol. 25, April 1996, pp. 448-476.
- [42] L. Trevisan, Reductions and (Non-)Approximability, Ph.D. Thesis, Dipartimento di Scienze dell'Informazione, University of Rome, "La Sapienza", Italy, 1997.
- [43] J.D. Ullman. Principles of Database and Knowledge Base Systems, Vols. I and II, Computer Science Press, Rockville, Maryland, 1989.
- [44] L.G. Valiant. The complexity of enumeration and reliability problems, SIAM J. Computing (SICOMP), Vol 8, No. 3, August 1979, pp. 410-421.
- [45] D. Zuckerman, On Unapproximable Versions of NP-Complete Problems. SIAM J. Computing, 25(6), pp. 1293-1304, 1996.